

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

FILED
JUN 19 2013
AT BALTIMORE
CLARK U.S. DISTRICT COURT
DISTRICT OF MARYLAND
ESPTV

IN THE MATTER OF THE APPLICATION)
OF THE UNITED STATES OF AMERICA)
FOR A SEARCH WARRANT FOR THE) Crim. No.
MICROSOFT, INC. ACCOUNT)
DOCKER42@HOTMAIL.COM)

13-1371SAG

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

I, Douglas Macfarlane, (your Affiant) Special Agent with the Federal Bureau of Investigation, Linthicum, Maryland, Major Case Coordination Unit, being duly sworn, hereby deposes and states as follows:

BACKGROUND OF AFFIANT

1. I have been employed as a Special Agent ("SA") with the Federal Bureau of Investigation (FBI) since April 1996, and I am currently assigned to the FBI's Violent Crimes Against Children Section, Major Case Coordination Unit ("MCCU"). I am currently investigating federal violations concerning child pornography and the sexual exploitation of children and have gained experience through training in seminars, classes, and everyday work related to these types of investigations. I have participated in the execution of numerous warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information.

2. As a federal agent, I am authorized to investigate violations of the laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for a search warrant for

JPM
2013R232

information associated with email account "docker42@hotmail.com" that is stored at a premises owned, maintained, controlled, or operated by Microsoft, Inc., an electronic communications / Internet service provider headquartered at 1 Microsoft Way, Redmond, WA 98052. The information to be searched is described in the following paragraphs and in Attachment B. There is probable cause to believe that evidence of violations of Title 18, U.S.C. § 2252A(a)(2) and (a)(5)(B) (use of a computer in or affecting interstate commerce to possess, receive, or distribute child pornography), will be found at the premises owned, maintained, controlled or operated by Microsoft, Inc. Therefore, the search warrant requires Microsoft Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the electronic account of docker42@hotmail.com, more particularly described in Attachment A.

4. This affidavit is requesting authority to search the electronic account described in Attachment A and seize all items listed in Attachment B as instrumentalities, fruits, or evidence of crime. Electronic accounts such as those maintained by Microsoft Inc. can contain stored electronic information including previously saved email conversations and instant message conversations along with any data files (e.g., images, videos, etc...) attached to these saved communications.

5. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence, fruits, or instrumentalities of the violations of Title 18, U.S.C. § 2252A(a)(2) and (a)(5)(B) including, but not limited to, the items described on Attachment B, which is attached hereto and incorporated herein by reference, are presently located at the premises described on

Attachment A, which is also attached hereto and incorporated herein by reference.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO COMMUNICATE
ONLINE AND CONSPIRE TO ADVERTISE, DISTRIBUTE
AND COLLECT CHILD PORNOGRAPHY**

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize internet forums to communicate and conspire with others to advertise, distribute, receive and collect images and videos of child pornography:

- a. Individuals who conspire with others to advertise, distribute and collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Individuals who conspire with others to advertise, distribute and collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Individuals who conspire with others to advertise, distribute and collect child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, individuals who conspire with others to advertise, distribute and collect child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years

and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

- e. Individuals who conspire with others to advertise, distribute and view child pornography correspond with and/or meet others to share information and materials rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- f. Individuals who would email others child pornography would have had to met those individuals in other online forums designed to attract those interested in child pornography. These individuals gain knowledge each other's email addresses through online communication with others of similar interest on forums. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have areas dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.
- g. Individuals who conspire with others to advertise, distribute and collect child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Users will maintain their collections both off and online.
- h. Individuals who conspire with others to advertise, distribute and collect child pornography often utilize the same online account(s), such as an e-mail account, for an extended period of time to collect and distribute child pornography material. One of the reasons for this is to establish the account(s) as being known to other collectors and distributors of child pornography to foster the individual's ability to obtain child pornography material. Similar investigations involving the distribution of child pornography materials via e-mail have routinely identified individuals who have utilized the same e-mail account(s) for an extended period of time; many times over a multiple-year period.
- i. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, collectors and distributors of child pornography often establish online accounts, such as e-mail accounts, that are distinct from accounts associated with their true identities. One of the reasons for this is to conceal their true identities from law enforcement.

PROBABLE CAUSE

7. In 2013, the FBI office in Eugene, Oregon was investigating an individual for child pornography offenses. Your Affiant received information about the investigation from Special Agent Jason Cherry ("SA Cherry") from the FBI Office in Eugene, Oregon. On March 26, 2013, a federal search warrant was executed at that individual's residence in Coos Bay, Oregon. In an interview with agents and officers during the search, this individual, who is known to law enforcement, admitted to possessing numerous images and videos of child pornography, and also gave consent for the FBI to take over his email account ("takeover account"). A subsequent review of this email account confirmed his admission.

8. SA Cherry later gave your Affiant the takeover account information for further investigation into other possible subjects trading child pornography using email. Your Affiant assumed control of the takeover account in an undercover capacity on or about March 27, 2013, in Linthicum, Maryland.

9. On April 16, 2013, your Affiant logged into the email account and found an email sent to the account from email address docker42@hotmail.com dated April 13, 2013. Attached to this email were several pictures of prepubescent females wearing only their underwear or bathing suits.

10. On April 16, 2013, your Affiant, working from an undercover computer in Linthicum, Maryland, sent an email from the takeover account to docker42@hotmail.com stating, "I'm not interested in softcore. Sorry." A few minutes later, docker42@hotmail.com replied with an email containing several pictures of child pornography. Specifically, there was a file named "boy man (16).jpg" which depicted an adult male performing oral sex on a

prepubescent boy. There was another file named "giry (47).jpg" that depicted a prepubescent female performing oral sex on an adult male.

11. On April 26, 2013, your Affiant sent an email to docker42@hotmail.com asking him if he has ever traveled to Asia or anywhere to have sex with minors. This began a conversation consisting of several emails back and forth on April 26, 2013 between your Affiant and docker42@hotmail.com. During this conversation, docker42@hotmail.com stated, "I went to Bangkok in 2011 for one week and it was great. Had two 9yo and a 10yo and they would do anything, cost me about 2000 for the week but, was well worth it." In another email, docker42@hotmail.com said that took pictures during his Thailand trip but asked your Affiant to send him some child pornography in exchange for these pictures.

12. On May 23, 2013, your Affiant received subpoena results from Microsoft, Inc. for docker42@hotmail.com and found that the account was created on March 5, 2013. Therefore, the contents of this account are sought from March 5, 2013, to present.

CONCLUSION

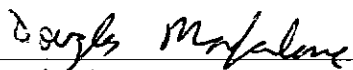
13. Based on the foregoing, I respectfully submit that there is probable cause to believe that Microsoft, Inc., 1 Microsoft Way, Redmond, WA 98052, maintains evidence in the account described in Attachment A to this affidavit of violations of 18 U.S.C. § 2252A(a)(2 and (a)(5)(B), receipt, distribution and possession of child pornography. This evidence, listed in Attachment B to this affidavit, which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

14. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

13-1371SAG

15. Pursuant to Title 18, U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

16. Pursuant to Title, 18 U.S.C. § 2705(b), your Affiant requests the Court order Microsoft, Inc. not to notify any other person of the existence of this warrant for the next ~~180~~⁹⁰ days. This request is made because the existence of the warrant will seriously jeopardize the ongoing investigation.


Special Agent
Douglas Macfarlane
Federal Bureau of Investigation

SUBSCRIBED TO AND SWORN BEFORE ME
THIS 5th DAY OF JUNE, 2013


HONORABLE STEPHANIE A. GALLAGHER
UNITED STATES MAGISTRATE JUDGE

13-1371SAG

ATTACHMENT A

ITEMS TO BE SEIZED AND SEARCHED

This warrant applies to information associated with the electronic account:

docker42@hotmail.com; which is stored at premises owned, maintained, controlled, or operated

by Microsoft, Inc., 1 Microsoft Way, Redmond, WA 98052.

13-1371SAG

ATTACHMENT B

SPECIFIC ITEMS TO BE SEIZED

I. Information to be disclosed by Microsoft Inc.

Microsoft Inc. is required to disclose the following information to the government for email account docker42@hotmail.com from March 5, 2013 to present:

1. The contents of all e-mails and instant messages stored in the account, including copies of e-mail and instant messages sent to and from the account, e-mail and instant message drafts, the source and destination e-mails and messages sent addresses associated with each e-mail and message, the date and time at which each e-mail and instant message was sent, and the size and length of each e-mail and instant message, attachments, including visual depictions of children clothed, partially clothed or engaged in sexually explicit conduct pursuant to 18 U.S.C. § 2256;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

4. All records pertaining to communications between docker42@hotmail.com and any person regarding these accounts, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence or instrumentalities of violations of Title 18, U.S.C. § 2252A involving electronic account docker42@hotmail.com, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

1. Communications to/from the electronic account docker42@hotmail.com or other electronic data (such as unsent communication drafts) contained in docker42@hotmail.com that demonstrate violations of Title 18, U.S.C. § 2252A.
2. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.